WHAT IS CLAIMED IS:

1. A method for authenticating a document and a presenter of the document, comprising:

obtaining, at a location whereby the document is being presented by the document presenter, information provided on the document that is to be used to authenticate the document, the information being encoded in a particular format;

decoding the information to obtain first data and second data, the first data corresponding to unencoded data written on the document to be used to verify whether the document has been modified, the second data corresponding to biometric data of the document owner to be used to verify whether the document owner corresponds to the document presenter; and

obtaining biometric data of the document presenter and comparing the biometric data of the document presenter to the second data,

wherein the document is authenticated if the second data matches the biometric data of the document presenter and the first data matches the written data obtained from the document.

2. The method according to claim 1, wherein biometric data corresponds to at least one of retinal scan data, fingerprint data, voiceprint data, and photographic data, or other viable biometric data set.

3. The method according to claim 1, wherein the decoding step includes the steps of:

obtaining a public key from the decoded information; and

validating the certificate by verifying the digital signature within the certificate that proves the validity of the public key contained therein.

4. The method according to claim 3, wherein the decoding step further includes the steps of:

performing a cryptographic algorithm on the first data and the second data to obtain biometric data of a document owner to be compared against the biometric data obtained from the document presenter.

5. A document authentication system, comprising:

a biometric capture unit that is configured to capture biometric information of a document owner;

a protected data capture unit that captures protected data of the document owner;

a digital signature unit that provides a digital signature of an entity;

a signed data block creation unit that combines the biometric information and the protected data, to provide a signed data block;

a security data block creation unit that combines the signed data block and the digital signature of the signed data block with a public key of a document issuer to create a biometric security data block; and

an encoding and output unit that encodes the biometric security data block into a particular format and outputs the encoded biometric security data block to the document,

wherein the biometric security data block is used by a document verifier to authenticate the document and to authenticate a presenter of the document with respect to the document owner.

6. The system according to claim 5, wherein the particular format is a bar code format.

7. A secure document creation and authentication system, comprising:

a first biometric capture unit that is configured to capture biometric information of a document owner;

a second biometric capture unit that is configured to capture biometric information of a document presenter;

a protected data capture unit that captures protected data of the document owner;

a digital signature unit that provides a digital signature of a document issuer that issues the secure document to the document owner by using a private key of the document issuer;

a signed data block creation unit that combines the biometric information of the document owner and the protected data of the document owner to provide a signed data block;

a security data block creation unit that combines the signed data block and the digital signature of the signed data block with the public key of the document issuer to create a biometric security data block; and

an encoding and output unit that encodes the biometric security data block into a particular format and outputs the encoded biometric security data block to the document,

wherein the biometric security data block is used by a document verifier to authenticate the document and to authenticate a presenter of the document with respect to the document owner by comparing the biometric information of the document owner obtained from the document with the biometric information of the document presenter as output by the second biometric capture unit.

8. The system according to claim 7, wherein the biometric data is at least one of retina eye scan, DNA information, fingerprint information, voiceprint information, and photographic information, or other viable biometric data set.